



Protecting DOE Office of Science Resources while Maintaining an Open Collaborative Science Environment

Deborah Agarwal (DAAgarwal@lbl.gov)
Dwayne Ramsey (DGRamsey@lbl.gov)
Horst Simon (HDSimon@lbl.gov)
Lawrence Berkeley Laboratory

1




Key Points

- Open science represents a challenging cybersecurity environment
- Open collaborative science has unique cybersecurity requirements
- Research and development is needed to address cybersecurity issues critical to secure open science
- DOE Office of Science labs are in a unique position to perform the research and development required


Dr. Orbach Briefing September, 2006

2

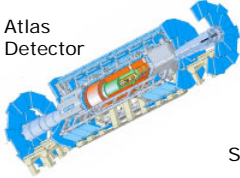


U.S. Department of Energy
Office of Science

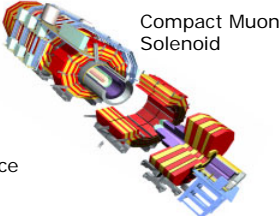
Large-Scale Open Collaborative Science



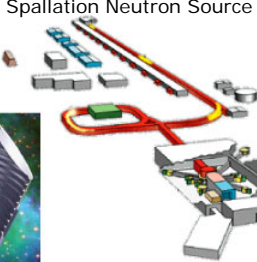
BERKELEY LAB




Atlas Detector



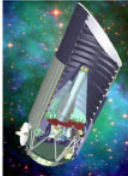
Compact Muon Solenoid



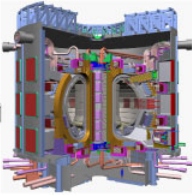
Spallation Neutron Source



Ultrahigh Voltage Electron Microscope




Supernova/Acceleration Probe



ITER Tokamak


Dr. Orbach Briefing September, 2006

3



U.S. Department of Energy
Office of Science

Open Science - Challenging Cybersecurity Environment




BERKELEY LAB

- Science collaborations can involve 1000's of scientists and distributed resources spread throughout the world
 - Greater than 50% of DOE Office of Science PIs and facility users are at universities
 - Greater than 85% of ESnet traffic is to and from universities and other non-DOE facilities
 - NERSC user population of around 2500 users (over 50% university)
 - 18 of the 20 top flows in ESnet are to or from a site outside the US
- Mission relies upon core capabilities of high performance computing, networking, and data transfers
- Many users never visit the site
- Virtual organization involved in managing the resources
- Users access resources from computers not under DOE control

Success of these collaborations depends on robust, open, and secure high-performance science infrastructure


Dr. Orbach Briefing September, 2006

4



U.S. Department of Energy
Office of Science

Open Science is on the Front Lines




BERKELEY LAB

- The techniques needed to protect the open science environment today are needed by other environments tomorrow – Past examples
 - Network intrusion detection
 - Insider threat
 - Defense in depth
 - High performance capabilities
- A next set of concerns
 - Reducing credential theft opportunities (e.g. PKI, passwords)
 - Detection of stolen credentials and insider attacks
 - Communication and coordination between components to recognize and react to attacks in real time
 - Tools which address vulnerabilities before they are exploited
 - Improved analysis techniques – data mining and semantic level searches
 - Prevention and detection of session hi-jacking


5

Dr. Orbach Briefing September, 2006



U.S. Department of Energy
Office of Science

Office of Science Laboratories as a Cybersecurity R&D Environment




BERKELEY LAB

- Staff
 - Expert cybersecurity and networking operations staff
 - Top cybersecurity researchers and developers
- Resources
 - Leading edge networking and computational environment
 - High performance and high value facilities and networks
- Cybersecurity
 - Challenging cybersecurity problem
 - Opportunity to test and gain experience with new capabilities in an operational setting
 - Unclassified environment
- Users and applications
 - Global and diverse user population
 - Many advanced custom applications that continually adapt
 - Significant cross site collaboration and data transfer

The lab environment brings together all of the above as a team


6

Dr. Orbach Briefing September, 2006





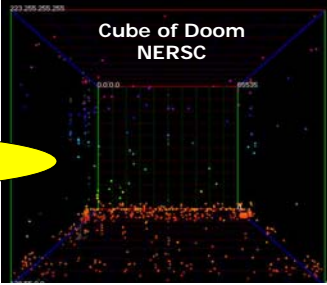
U.S. Department of Energy
Office of Science

Berkeley Lab Cyber Approach



Effective cyber security requires research, development, and operations integration

- **Create tools to gather/analyze data**
 - Observe and understand the cyber universe
 - Adapt our protection mechanisms to the behavior of that universe (*monitor, detect, notify, resolve*)
- **Competent staff motivated by both research and operations**
 - Researchers challenged by real world problems
 - Operations staff stimulated by research discoveries
- **Operations**
 - Cyber Protection has **oversight** over the full range of computer security activities at Berkeley Lab


Research

Berkeley Lab
Computer
Protection Program

Protection


Dr. Orbach Briefing September, 2006

7



U.S. Department of Energy
Office of Science

The Reality of Cyber Security Operations




- **No perfect protection**
 - Miscreants are relentless, passionate and creative - always developing new attacks
 - Constantly need to improve our protection (no false sense of security)
- **Open science needs different protection than military, business, and government**
 - Scientific collaborators are full partners, not guests
 - Diverse computing environment feeds research
 - DOE Office of Science can make a contribution to the larger R&E community
- **Collaboration between research and operations creates**
 - Stimulating intellectual environment
 - Continuous challenges

Spurs our Cyber protection program to be more relentless, passionate, and creative than the attackers.


Dr. Orbach Briefing September, 2006

8



U.S. Department of Energy
Office of Science


LBL Incident Response based on Research



BERKELEY LAB


- We understand Internet traffic better than most sites because of Bro
 - >27 billion connection records on hand (all LBL Internet connections since 1994)
- Defense in depth examples:
 - **Boyz from Brazil (Case 216)** - Detect by Bro, custom sensor deployed to hosts (Bondo)
 - **Malicious Code** - Detect by Scanning, Jail hosts with NETS
 - **Case 632** - Scan Active Directory, Monitor outbound DNS traffic with custom code
 - **"SirVic" (recent math hack) Ivy League, UCB, et. al;** - LBL forensics identifies scope, Incident Team alerts other victims + CIAC, CERT. Assists DOE Cyber Crimes, helps locate miscreant.

9




U.S. Department of Energy
Office of Science

A Suggested Office of Science Cybersecurity Strategy



BERKELEY LAB



- Monitor and react – restrict only when necessary
 - Provide a balance between openness and security
 - Only block disallowed and malicious traffic
- Defense in depth
 - Secure systems from the inside out
 - Protections for each resource specific to the vulnerabilities of the resource and the potential impact of a compromise
- Vulnerability testing and patching of science software
- Technologies
 - Use off-the-shelf technology when possible but often does not meet needs
 - Perform the research and development needed to fill the gaps and provide world-class cybersecurity to DOE Office of Science
- Team research, development, and operations staffs to ensure that solutions are relevant to DOE Office of Science needs and environment

Create an intellectual and innovative cybersecurity environment
Address the spectrum of operational and long-term research needs.
Stay ahead of the next incident

10



U.S. Department of Energy
Office of Science

An R&D Agenda to Protect High Performance Open Science




BERKELEY LAB

- Coordination between cybersecurity components and across sites
 - Border and ESnet intrusion detection mechanisms (10 Gbit and higher)
 - Site internal network intrusion detection mechanisms
 - Host security mechanisms
 - Software authentication and authorization mechanisms
 - Cross-site detection of concerted and coordinated attacks
- Authentication mechanisms for users who never physically visit the site
- Efficient forensics information collection and correlation
- Analysis tools for cybersecurity data particularly in a high-performance environments
- Improved recovery capabilities – it is currently weeks to recover a supercomputer
- Cybersecurity as an integral consideration in building middleware
- Funded deployment and support activities


A new operations oriented Cybersecurity R&D effort is needed to help protect open science

11



U.S. Department of Energy
Office of Science





DOE –Researchers and Operations Working Together



BERKELEY LAB

Example Past Successes:

- Bro – network intrusion detection
- Network telescope
- Honey Pots and Farm
- Federated radius
- One-time password
- Cube of Doom
- NETS

12

Conclusions

- Open collaborative science has become core to the mission of the Office of Science
- We need cybersecurity that doesn't inhibit collaborative science
- ***Cybersecurity for open science introduces cybersecurity challenges well beyond the state-of-the-art in the typical commercial and government environments***
- ***Need to partner cybersecurity operations, cybersecurity researchers, system administrators, and developers***